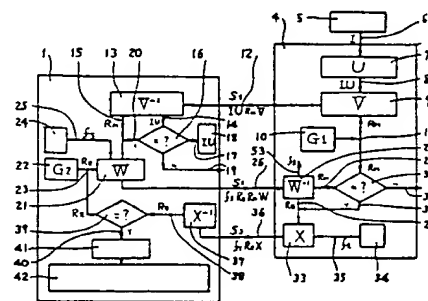


(54) IC CARD SYSTEM

(11) 63-184164 (A) (43) 29.7.1988 (19) JP
 (21) Appl. No. 61-188186 (22) 11.8.1986
 (71) HIKARI YOKOEKAWA (72) HIKARI YOKOEKAWA
 (51) Int. Cl. G06F15/21, G06F15/30, G06K17/00

PURPOSE: To decide the justifiability of a main device and a card, by sending a data including a random number from the main device side and the card side to an opponent side to each other, returning it to a transmission side after processing at the opponent side, and collating it with an original random number.

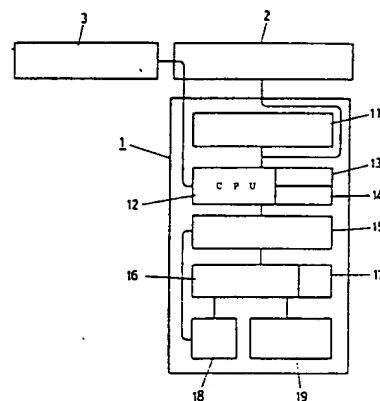
CONSTITUTION: At the main device 4, a signal IU converted from an inputted identification I at conversion U8 is sent to the random number R_M of a random number generator 10 and the card 1 converted at conversion V9. At the card 1, the signal IU and the random number R_M are recovered and separated at reverse conversion V⁻¹13, and at a collator 16, the signal IU is collated with the identification data of an identification data storage 18. When both coincide, the random numbers R_E and R_M of a random number generator 22 are converted at conversion W21, then, they are sent to the main device 4. At the main device 4, the random numbers R_M and R_E are recovered and separated at reverse conversion W⁻¹27, and the random number R_M is collated with the original random number R_M at a collator 30, and when they coincide, the random number R_E is converted at conversion X33, and is sent to the card 1. At the card 1, when the random number R_E recovered at reverse conversion X⁻¹37 coincides with the original random number R_E , access to a memory zone 42 is permitted.

**(54) PORTABLE PRODUCT DATA PROCESSOR**

(11) 63-184165 (A) (43) 29.7.1988 (19) JP
 (21) Appl. No. 62-15098 (22) 27.1.1987
 (71) FUAMIRII MAATO K.K.(2) (72) HITOSHI SAKUMA(2)
 (51) Int. Cl. G06F15/24, G06K7/10, G07G1/00

PURPOSE: To easily perform the ordering and the stock control of a product, by providing a wand scanner which reads the product code of the product and a product data corresponding to the product code in a portable device.

CONSTITUTION: First of all, the product code read from the bar code of the product by the wand scanner 3 is inputted to the CPU12 of a main body 1, and the product data such as the product name, the optimum stock quantity, etc., of the product corresponding to the product code is read out from a file memory 15, and is displayed on a display part 11. At this time, by inputting a preset stock quantity from a keyboard 16, an ordering quantity is calculated from the data of the optimum stock quantity included in the product code and the data of the present stock quantity, and a calculated result (ordering quantity) is stored in the file memory 15. And after performing such work on every product, the ordering quantity of each product stored in the file memory 15 is printed out with a printer unit 2.



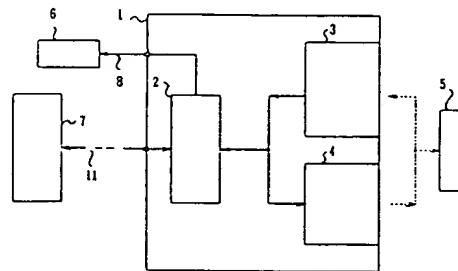
11: LCD display part, 13: OS memory, 14: program memory, 17: buzzer, 18: backup battery, 19: battery package

(54) AUTOMATIC REPAYMENT DEVICE FOR VOTING TICKET

(11) 63-184166 (A) (43) 29.7.1988 (19) JP
 (21) Appl. No. 62-16724 (22) 27.1.1987
 (71) FUJITSU LTD (72) YOICHI HIRASAWA
 (51) Int. Cl. G06F15/28, G07D9/00

PURPOSE: To prevent the exerciser of an unauthorized pari-mutuel ticket from escaping and to prevent the recurrence of malfeasance from occurring, by informing the fact of a repayment request by the unauthorized pari-mutuel ticket to a competition manager without being recognized by a repayment requesting person.

CONSTITUTION: When the repayment requesting person 5 inserts a pari-mutuel ticket to an automatic repayment device 1 for a voting ticket, the content of the ticket is read by a voting ticket processing part 3, and a read data is sent to a central processor 7 by a control part 2 via a communication line 11. The central processor 7 refers the described content of the pari-mutuel ticket to the result of a corresponding race, then, decides a refund money, however, when it is found that the pari-mutuel ticket is a forged or altered ticket, the information of the detection of the malfeasance is returned to the device 1. And the device 1 receiving the information of the detection of the malfeasance makes a money processing 4 operates as if normal repayment is performed to the repayment requesting person 5, and also, the information is sent with an alarm means 6 only recognizable by the competition manager.



⑫ 公開特許公報(A)

昭63-184164

⑬ Int. Cl.⁴G 06 F 15/21
15/30
G 06 K 17/00

識別記号

3 4 0
3 4 0

庁内整理番号

C-7230-5B
7208-5B
T-6711-5B

⑭ 公開 昭和63年(1988)7月29日

審査請求 未請求 発明の数 1 (全5頁)

⑮ 発明の名称 ICカードシステム

⑯ 特 願 昭61-188186

⑰ 出 願 昭61(1986)8月11日

⑱ 発 明 者 横 江 川 光 東京都足立区東綾瀬2-5-2-401

⑲ 出 願 人 横 江 川 光 東京都足立区東綾瀬2-5-2-401

明 細 書

1 発明の名称 ICカードシステム

2 特許請求の範囲

主装置が乱数 R_n 又は R_n を含むデータを送り、カードで加工ののち主装置に戻す α 環状路と、カードが乱数 R_e 又は R_e を含むデータを主装置に送り、主装置で加工ののちカードに戻す β 環状路を併設したICカードシステム。

3 発明の詳細な説明

本発明は、カードの改ざんや偽造、主装置の不正作成使用を防止するICカードシステムに関する。従来のICカードシステムでは、使用中のカード端子から盗聴等を得た信号を記録し、うちにこの信号を再利用する不正使用への対策がなかった。本発明は、ICカードシステムに、主装置が乱数 R_n 又は R_n を含むデータを送り、カードで加工ののち主装置に戻す α 環状路と、カードが乱数 R_e 又は R_e を含むデータを主装置に送り、主装置で加工ののちカードに戻す β 環状路を併設する。たとえば、主装置に発生させた乱数 R_n を変換又

は少くとも R_n を含む1組の値を合体変換した信号 S_1 をカードへ送り、カードが S_1 から復元した R_n 又は復元 R_n にもとづく変換値を信号 S_2 又は S_2' として主装置に返送し、さうにカード内に発生させた乱数 R_e を変換又は少くとも R_e を含む1組の値を合体変換した信号 S_3 又は S_3' を主装置へ送り、主装置が、復元した R_e 又は復元 R_e にもとづく変換値を信号 S_3 としてカードに返送する、ICカード、主装置、及びそれらより成るICカードシステムを構成する。

α 環状路は、主装置からカードに信号 S_1 を送る往路と、カードから主装置に信号 S_2' を返す復路と、 β 環状路は、カードから主装置に信号 S_2 を送る往路と、主装置からカードに信号 S_3 を返す復路を持つ。 α と β を独立に構成する他、 S_2' と S_2 を S_2 にまとめた、一部共有の構成も可能である。

β 環状路の復路信号 S_3 を用いた照合結果にメモリゲート駆動を行う構成とする。また、 α 環状路についてはカード内に2行い変換処理の結果が、 β 環状路については主装置内に2行い変換処理の

結果が、とちとち反映される復路信号とする。よって、復路信号を往路信号と異なるデータ形式に構成する。さらに、信号に複数の情報を混載しうる。例えば、往路の往路信号 S_1 にて、乱数 R_n の他に暗証 I やその変換 IU はじめ、パスワードやファイルキー、口座番号など f コードを混載できる。この際送信中の盗聴防止のため、複数の情報の合体変換加工を行う。ある環状路で運んだ f 等と、他の環状路に入力して処理、照合、同期等に用いる構成も可能である。

オ1図は本発明のICカードシステム構成図にて、少くともIC外部からのアクセス不能メモリ⑫や制御プログラム⑬とCPU⑭をもつ主回路①を設置した、端子⑭つきICカード②及び、当該ICカードと読出し書き込み及びデータ処理を行う主装置③より、ICカードシステムが構成される。主回路①は、ワンチップIC又は数個のICにて実現する。主装置③は、少くとも外部からのアクセス不能メモリ⑭や制御プログラム⑮とCPU⑯をもつ主回路④を

搭載する。主回路④はワンチップICや複数個のICをアセンブルしてブラックボックス化した集合体にて実現する他、主回路の代用として別のICカードを組み込んで用いることもできる。

オ2図は、本発明の実施例の処理の流れを示す。キー入力部⑤より入力の暗証 I ⑥を変換 U ⑦にて IU ⑧に変換のち変換 V ⑧に入力する。⑧は主装置内の乱数発生部 G_1 ⑩で発生させた乱数 R_n ⑪と IU ⑧とを合体変換加工して信号 S_1 ⑫をつくり、カードに送る。 S_1 のフォーマットを IUR_nV にて示す。 IU と R_n の順序は任意でよい。カード内にて、逆変換 V^{-1} ⑬が復元 IU ⑭と復元 R_n ⑮を復元分離する。照合部⑯は⑭と、識別データ格納部⑰より取出した識別データ IU ⑱と比較照合し、不台致⑲なら排除し、台致⑳なら使用者と主装置が正当と判定して⑮を変換 W ㉑に送るのを許可する。㉑はカード内の乱数発生部 G_2 ㉒で発生させた乱数 R_e ㉓と、 f 格納部⑳から取出したコード f_1 ㉔とを合体変換加工して信号 S_2 ㉕をつく

り、主装置に送る。 S_2 のフォーマットを $f_1R_eR_nW$ にて示す。 f_1 、 R_e 、 R_n の順序は任意でよく、また f_1 は省略してもよい。主装置内にて、逆変換 W^{-1} ㉖が復元 R_n ㉗と復元 R_e ㉘を復元分離する。照合部⑳は㉘と、もとの乱数 R_n ⑪と比較照合し、不台致㉙なら排除し、台致㉚ならカードを正当と判断して㉙を変換 X ㉛に送るのを許可する。㉛は㉙と、 f_1 格納部㉔より取出したコード f_1 ㉔とを合体変換加工して信号 S_3 ㉜をつくり、カードに送る。 S_3 のフォーマットを、 f_1R_eX にて示す。 f_1 、 R_e の順序は任意でよく、また f_1 は省略もできる。

カード側にて、逆変換 X^{-1} ㉞が S_3 ㉜から復元 R_e ㉟を分離し、照合部㉙にて㉟と、もとの乱数 R_n ㉗と比較照合の上、台致㉚すればメモリゲート㉡をオープンし、メモリゾーン㉢へのアクセスを許可する。

このように、カード側の照合部⑳にて復元 IU ⑭をチェックするので使用者と主装置の両方の正当性をカードが判定でき、一方主装置側では、も

との R_n に対し主装置及びカードにて変換と逆変換をくり返した結果に得る R_n を主装置に還元させ、もとの R_n と比較照合することで、カードの正当性を判定できる。

上記にて、もしカード内で発生させた乱数 R_e を用いず、主装置がカードに R_e を含め信号 S_2 を送る構成とすると、信号の盗聴再利用を許してしまい不都合である。たとえカードを正常使用中に端子から S_2 と S_3 信号を盗聴記録しておき、やちに正当でない主装置を用いて盗聴した S_2 信号をカードに入力すれば不正にカードを起動でき、カードより送られる S_2 や S_3 信号をよみとばして、盗聴した S_3 信号を入力すれば、不正の主装置にてメモリへのアクセスが可能としてみよう。他人や自分自身のカードの顔面改ざん等を可能としてみよう。

そこで、カードにて R_e を発生させ、 R_e 又は少くとも R_e を含む値の変換値をカードから主装置に送り、主装置は受けた R_e の変換値又は少くとも R_e を含む値の変換値を信号 S_3 としてカードに返送し、カードにて復元した R_e と、もとの発信した R_e と比較

照合して合致時にのみメモリゲートをオープンするよう構成すれば、主装置がたしかにカードから先刻発信された Re にもとづき S_1 を作成したと確認できる。よって、盗聴しおいた S_1 をカード入力しても、使用した Re 値がその都度異なるため、照合は成立せず、メモリアクセスできない。即ち、信号の盗聴再利用を防止できる。

合体変換する信号は、送信途上での盗聴解読防止のためであり、さらに複数個のデータをからみあわせて送ることによって互にカムフラージュすると共に一度に送信できるゆえ、カードと主装置間の送受信回数を減少できる。合体変換した結果のフォーマット、例えば $f_5 Re R_n W$ という表示は、 f_5 は Re 、 R_n といったコードや値を、手順 W を用いて変換処理した出力を示す。一例として

f_5	0 1 0 1 0 0 1 1
Re	1 1 0 1 0 1 1 0
R_n	1 0 1 0 1 1 1 0

とし、 W 手順を

① f_5 をビット反転

識別データとして IU のかわりにパスワード等 f_4 を暗証入力 I と組合せて用いる際は、 α 3図に示すように構成し、信号 S_1 のフォーマットを $f_4 I R_n V$ とすればよい。

α 4図に信号のフォーマット例を示す。 α 4図(a)にて S_1 のフォーマットは $f_4 I U R_n V$ あるいは $f_4 I R_n V$ 、 S_2 のときは $f_3 R_n W$ となる。 $W=V$ 、 $f_3=f_4$ も可能である。 S_2 のときは $f_2 Re$ あるいは $f_2 Re Y$ となり、 Y は変換を示す。 $Y=V$ 、 $Y=W$ も可能である。 f_2 は省略できる。 S_3 のフォーマットは $f_2 Re X$ であり、 f_2 は省略できる。

α 4図(b)は、 Re と R_n をひとりの信号内に組込で構成の例で、 S_1 、 S_3 のフォーマットは α 4図(a)と同じであるが、 S_2 のときは $f_5 Re R_n W$ となる。 $W=V$ 、 $f_4=f_5$ も可能である。

⑤1が α 環状路、⑤2が β 環状路を示す。

⑤3は選送し復元した f_5 、例えば口座番号等である。

⑤4 Re の上4ビットと、⑤5を施した f_5 の下4ビットを交換

⑤6 R_n の上4ビットと、 Re の下4ビットを交換

⑤7 R_n の下4ビットと、⑤5を施した f_5 の上4ビットを交換

⑤8 以上の順に2進した3バイトを合体して信号 S_2 とする

とすれば、 S_2 は16進表示で EDC A6 A が生成される。さらに、 f_5 のバイト数を増加させ、秘密度を高める。2、 W^{-1} 手順は、上記 W 手順の逆プロセスとなる。

主装置に設けた変換 U は、主装置が不正目的で盗まれたり、秘密が洩れた時の暗号更新と円滑に行うための構成で、主装置を更新する際は変換 U

⑦を更新するのみでよい。カード使用者には、必ず本人確認のうち、入力された I をもとに新 IU を作成して識別データ格納部を更新するのみでよい。

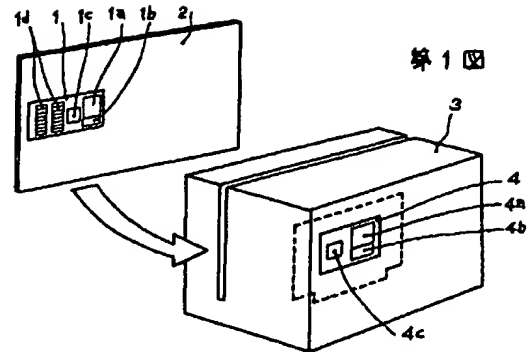
f には、パスワード、ファイルアクセスキーや其他任意の値、コードを採用しうる。

4 図面の簡単な説明

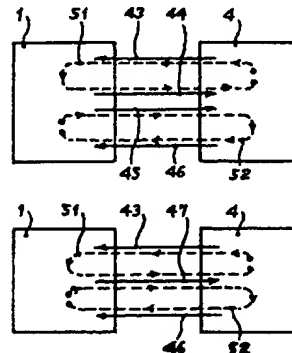
α 1図は本発明のカードシステムの構成図、 α 2図と α 3図は実施例の処理のながれを、 α 4図は信号のフォーマットを示す。

1…カードの主回路、1a…外部からアクセス不能メモリ、1b…制御プログラム、1c…CPU、1d…端子、2…ICカード、3…主装置、4…主装置の主回路、4a…外部からアクセス不能メモリ、4b…制御プログラム、4c…CPU、5…キー入力部、6…暗証 I 、7…変換 U 、8… IU 、9…変換 V 、10…乱数発生器 G_1 、11…乱数 R_n 、12…信号 S_1 、13…逆変換 V^{-1} 、14…復元 IU 、15…復元 R_n 、16…照合部、17…識別データ格納部、18…識別データ IU 、19…不合致、20…合致、21…変換 W 、22…乱数発生器 G_2 、23…乱数 Re 、24… f_5 格納部、25…コード f_5 、26…信号 S_2 、27…逆変換 W^{-1} 、28…復元 R_n 、29…復元 Re 、30…照合部、31…不合致、32…合致、33…変換 X 、34… f_2 格納部、35…コード f_2 、

36...信号 S_3 , 37...逆変換 X^{-1} , 38...復元 RE ,
 39...照合番, 40...合致, 41...メモリバート,
 42...メモリゾーン, 43...信号 S_2 , 44...信号 S_2' ,
 45...信号 S_2'' , 46...信号 S_3 , 47...信号 S_2 ,
 48... f_4 格納番, 49...コード f_4 , 50...信号 S_1
 51... α 環状路, 52... β 環状路
 53...復元 f_5



第1図



第4図
[a]

[b]

特許出願人 横江川 光

手続補正書

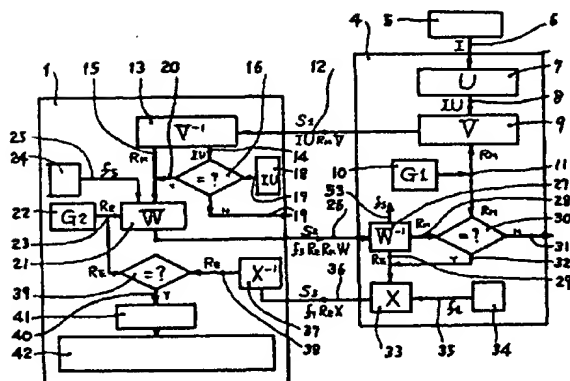
昭和62年11月10日

特許庁長官 殿
 (特許庁審査官 殿)
 1. 事件の表示 昭和61年 特許願第188186号
 2. 発明(考案)の名称 ICカードシステム
 意匠に係る物品
 指定商品および商品の区分 第 類

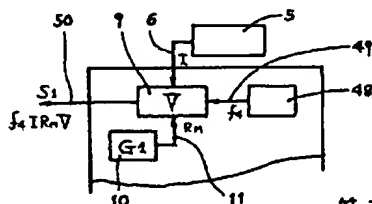
3. 補正をする者 事件との関係 特許出願人
 住所 郵便番号 112-0000
 東京都足立区東横須賀 2-5-2-401
 氏名 (本人にあっては署名および氏名、代理人にあっては署名および氏名) 横江川 光

4. 補正命令の日付 昭和 年 月 日

5. 補正の対象 明細書の発明の詳細な説明欄
 6. 補正の内容 別紙のとおり



第2図



第3図

補正の内容

- 1 オ8頁 オ19行目
「 f_1 には、」 とあるを、
「 f_1 や f_5 などには、」 に補正。

- 2 オ10頁 オ20行目 ✓
「34... f_2 格納部」 とあるを、
「34... f_1 格納部」 に補正。

- 3 オ8頁 オ20行目の後に以下を挿入。

「いま S_1 と S_2 の往復にて、主装置と使用者が正当と確定できたとして、例えばカードのメモリー④にデータをかきこみたいとき、カード側に書き込みを告げるコード f_1 ⑤を用いるが、このとき対象のアドレスや書き込むべきデータなどを f_1 に添え又は連結して f_1' となし、 f_1' $R_n X$ のフォーマットの S_3 をカードに送り、カードが X' ⑦にて R_n ⑥を復元時に f_1' も復元しておき、 R_n 照合合致⑩のとき f_1' を処理して書き込みを

実行させればよい。このとき、複数の S_3 を発信することと告げる f_1 を用いた S_3 を1個、先ず発信し、フいでデータを f_1 としてのせた S_3 を告げた個数だけカードに送ることにて、多量のデータを一斉にカードに送りこめる。

カード側にて書き込みが正常に完了すれば、それを通知するコード f_5 を再び S_2 の発信にて、主装置側に通知することもできる。即ち、信号のやりとりは S_1 、 S_2 、 S_3 、 S_2 と続き、このように α 環状路と β 環状路を何度もくり返して交信ができる。この一連の交信時に、同一の R_n や R_e を用いてもよく、又例えば1回の交信毎に異なる乱数を用いてもよい。このとき、 S_3 のフォーマットとして S_2 のフォーマットと類似の $f_1 R_n X$ を用いれば、1回毎に異なる乱数による α 、 β 両環状路の連続交信が可能になる。カードのメモリー④からの多量データ読み出しも、この α 、 β の連続にて扱受できる。」

手続補正書

昭和63年3月1日

特許庁長官
(特許庁審査官)

殿
(殿)

1. 事件の表示
昭和61年 特許 願 第188186号
2. 発明(考案)の名称 ^{特許} ICカードシステム

3. 補正をする者
事件との関係 特許 出願人

住所 郵便番号 112-0000

東京都足立区東綾瀬2-5-2-401 03-666-7103

氏名 ^{特許} (特許人によっておおよそ) 横江川 光雄

4. 補正命令の日付 昭和63年2月2日

5. 補正により増加する請求項の数

6. 補正の対象 昭和62年11月10日提出の特許補正書の「補正の対象」の欄

7. 補正の内容 別紙のとおり

特許
63.3.1
正誤

手続補正書

昭和62年11月10日

特許庁長官
(特許庁審査官)

殿
(殿)

1. 事件の表示
昭和61年 特許 願 第188186号
2. 発明(考案)の名称 ^{特許} ICカードシステム

3. 補正をする者
事件との関係 特許 出願人

住所 郵便番号 112-0000

東京都足立区東綾瀬2-5-2-401

氏名 ^{特許} (特許人によっておおよそ) 横江川 光雄

4. 補正命令の日付 昭和 年 月 日

5. 補正により増加する請求項の数

6. 補正の対象 明細書の発明の詳細な説明の欄
明細書の図面の簡単な説明の欄

7. 補正の内容 別紙のとおり